CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1, 2, 5-12, 15-22, 25, and 26.
- After this Amendment: Claims 1, 2, 5-12, 15-22, 25, and 26.

Non-Elected, Canceled, or Withdrawn claims: 3, 4, 13, 14, 23 and 24

Amended claims: 1, 11 and 21.

New claims: none

Claims:

1. (Currently Amended) A method for use in a computer capable of supporting multiple authentication mechanisms, the method comprising:

generating at least one indicator that identifies a user, and is associated with and identifies at least one authentication mechanism that has been used to authenticate the user, wherein generating the indicator further includes identifying within the indicator at least one characteristic associated with the authentication mechanism, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism, wherein the measure of strength of the authentication mechanism depends on the length of key employed in an encryption process; and

controlling the user's access to at least one resource based on the indicator.

2. (Original) The method as recited in Claim 1, wherein generating the indicator further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism.

3. (Canceled).

4. (Canceled).

5. (Previously Presented) The method as recited in Claim 1, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

6. (Original) The method as recited in Claim 1, wherein controlling access to the resource based on the indicator further includes comparing the indicator to at least one access control list having at least one access control entry therein.

7. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is allowed to proceed.

8. (Original) The method as recited in Claim 6, wherein if the access control entry operatively specifies that the at least one authentication mechanism is not permitted to access the resource, then access to the at least one resource is not allowed to proceed.

9. (Original) The method as recited in Claim 6, wherein if the access control entry does not operatively specify that the at least one authentication mechanism is permitted to access the resource, then access to the at least one resource is not allowed to proceed.

10. (Original) The method as recited in Claim 1, wherein the indicator includes a security token.

11. (Currently Amended) A computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising:

producing at least one indicator that identifies a user, and uniquely identifies at least one authentication mechanism supported by the device that has been used to authenticate the user, wherein producing the indicator further includes identifying within the indicator at least one characteristic of the authentication mechanism, wherein the at least one characteristic of the authentication mechanism includes a strength characteristic of the authentication mechanism, wherein the strength characteristic of the authentication mechanism depends on the length of key employed in an encryption process; and

causing the device to selectively control the user's access to at least one resource operatively coupled to the device based at least in part on the indicator.

12. (Original) The computer-readable medium as recited in Claim 11, wherein producing the indicator further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism, in response thereto.

13. (Canceled).

14. (Canceled).

15. (Previously Presented) The computer-readable medium as recited in Claim 12, wherein the strength characteristic identifies a length of an encryption key employed by the authentication mechanism.

16. (Original) The computer-readable medium as recited in Claim 11, wherein causing the device to selectively control access to the at least one resource based on the indicator further includes causing the device to compare the indicator to control data.

17. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data specifies that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is allowed.

18. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data operatively specifies that the authentication mechanism is not permitted to access the resource, to which subsequent access to the resource is prohibited.

19. (Original) The computer-readable medium as recited in Claim 16, wherein if the control data does not operatively specify that the authentication mechanism is permitted to access the resource, to which subsequent access to the resource is prohibited.

20. (Original) The computer-readable medium as recited in Claim 10, wherein the indicator includes a security token.

21. (Currently Amended) An apparatus comprising:

at least one authentication mechanism ~~configured to generate~~ facilitating generation of at least one indicator that identifies a user, and identifies the authentication mechanism that has been used to authenticate the user, wherein the indicator further includes at least one identifying characteristic associated with the authentication mechanism, wherein the at least one identifying characteristic associated with the authentication mechanism indicates a measure of strength of the authentication mechanism, wherein the measure of strength of the authentication mechanism depends on the length of key employed in an encryption process;

an access control list;

at least one access controlled resource; and

logic operatively ~~configured to compare~~ facilitating comparison of the indicator with the access control list and selectively control the user's access to the resource based on the indicator.

22. (Original) The apparatus as recited in Claim 21, wherein the authentication mechanism is further configured to receive user inputs and generate at least one security identifier (SID) that identifies the authentication mechanism based on the user inputs.

23. (Canceled).

24. (Canceled).

25. (Previously Presented) The apparatus as recited in Claim 21, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

26. (Previously Presented) The apparatus as recited in Claim 21, wherein the indicator includes a security token.